

ENCRYPTED MEDIA KEY MANAGEMENT

FIELD OF INVENTION

This invention relates to the secure distribution of digitised audio-visual works using an encryption key management system.

PRIOR ART

Audio-visual entertainment works are conventionally distributed direct to the consumer by audio or video CDS or by broadcasting or cablecasting. Subject to adequate bandwidth the Internet provides a viable alternative for the distribution of digitised audio-visual works. Among other things digital distribution via the internet provides a solution to the problems which have hitherto hindered the development of video on demand services.

Technology for digitising and playing digitised audio and video works is well known. Where the digitised works are distributed electronically through a data network such as the Internet the size of the files (even when compressed) and the bandwidth of the network mean that streaming techniques must be used if the consumer is to be able to commence listening or viewing within a reasonable period of requesting the work to be downloaded. An example of streaming software is Real Networks Inc's RealServer and RealPlayer.

One of the problems with making available digitised audio-visual works on the Internet is that pirated copies may easily be made and distributed thereby depriving producers and copyright owners of income. There is a need to ensure that audio-visual works can be played only by consumers who have paid for them.

To control unauthorised use of Internet-distributed audio and video works encryption systems have been proposed, but the management of the keys required for decryption to date is inconvenient, inefficient or inadequate.

SUMMARY OF INVENTION

It is therefore an object of the present invention to provide a method for the secure distribution of digitised audio-visual works over a data network.

Accordingly in one aspect the invention consists in a method for the secure distribution of digitised audio-visual works ("media") to consumers over a data network comprising the steps of:

encrypting said media using a different encryption key for each work ("media key"),

storing the encrypted media on one or more first servers,

storing the media keys on a second server,

making available one or more retail servers from which consumers may obtain the right to receive media keys for desired media in exchange for complying with conditions set by the retailer,

the consumer causing a request to be made from a network-connected client device to a selected retail server for at least the media key for a desired media work,

at the selected retail server, verifying the consumer has complied with the retailer's conditions, and if so,

the retail server either passing said request to the second server, or supplying to the client device data allowing the second server to be contacted,

at said second server verifying the allowability of fulfilling requests from said retail server or a client device and if so allowable encrypting the relevant media key and downloading it to either said retail server or said client device,

said retail server if receiving an encrypted media key from said second server, downloading said encrypted media key to said client device,

at the client device decrypting the received media key and storing it in memory,

at the client device generating a request to the appropriate first server to supply the desired media work,

from the first server downloading the desired encrypted media work to said client device, and

at the client device retrieving the media key from said memory and using it to decrypt the media work to a condition where it can be played using appropriate player software.

The inventive concept may also be applied to the secure distribution of other digitised products over the Internet. Accordingly in a further aspect the invention

consists in a method for the secure distribution of digitised products to consumers over a data network comprising the steps of:

encrypting said products using a different encryption key for each product ("product key"),

5 storing the encrypted product on a first server,
storing the product keys on a second server,
creating steering files corresponding to each product and its corresponding key,
said steering files containing information identifying the media work and the
respective locations of the product and product key,

10 making available on a third server steering files corresponding to each product
for consumers to purchase,

said steering files when executed on a network-connected client computer device
accessible to the consumer causing a request to be made to said second server for the
key for the product identified in the steering file,

15 at the second server encrypting the relevant product key with a key unique to the
consumer and downloading it to said client device,

decrypting the product key at said client device and storing it in memory,

generating a request to the first server from said client device to deliver the
product identified in the steering file,

20 downloading the encrypted product from said first server to said client device,

retrieving the product key from said memory and using it to decrypt the product
to a condition where it is ready for use.

25 Preferably a public key encryption system is used to encrypt the media key for
downloading to the client device and to facilitate this the client device uploads to the
second server the consumer's public key.

BRIEF DESCRIPTION OF THE DRAWING

Figure 1 shows a diagrammatic representation of a key management system for encrypted digitised audio-visual works.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention in particular, but not solely concerns the secure online delivery of content such as audio-visual works in streaming media form. The content is encrypted and a key management or rights management system established to ensure only authorised users can decrypt and play the content. It is part of the invention that the encrypted content is made available separately from the encryption keys or access rights and these rights or keys are purchased or otherwise acquired by consumers from an entity who holds neither media or keys. Additionally security is maximised if all three functions are managed by separate entities from separate server sites.

The present invention delivers media keys to consumers or end-users who wish to have access to encrypted media through the use of client devices consisting of either general purpose computers (eg "PCS") or special-purpose computing devices (eg "set-top boxes") equipped with decryption processing capability. The encrypted media may consist of streams or of files. In this case wherein it is intended to be able to deliver the media to more than one recipient, whether simultaneously (multicast) or separately on a per-recipient basis (unicast), or else by a file download mechanism, an encrypting entity will perform the encryption using a media key generated for this purpose, and it is this media key that is to be delivered only to authorised end users. In the event that a public-key algorithm is used to encrypt the media, the term "media key" in this context is intended to mean the private key or decryption key required to decrypt the media.

In the systems described here, the media key is delivered to end users by an agent or entity termed a "key server". Following encryption of the actual media by the encrypting entity, the media key is transmitted or delivered securely to the key server. The encrypting entity also transmits or delivers the encrypted media, using any ordinary means, to a "media server" whose role is to deliver the media to end users either by multicast or unicast streaming or by a file download mechanism. More than one media server may be employed by the content provider. To best secure the media it is important for the key server and media server to be managed by separate entities.

An example of currently available means by which media streams may be delivered from a media server to an end user is the RealServer and RealPlayer software produced by Real Networks Inc.

Referring to Figure 1 in one embodiment of the proposed system for delivering media keys "just in time" for their use, an end user will obtain from a retailer 11 (i.e. an Internet "store" or "shop") by making a request 12, a "steering file" 1 for the media work selected by the user which is downloaded 13 to the user. This file contains information needed by the user's software running on client device 10 to make two requests: one for the appropriate media key, and the other for the user selected encrypted media. The latter function may be omitted in some business models with the user obtaining encrypted media independently of and at a different time to obtaining the media key. The retail store 11 will have previously downloaded or updated 16 a database 14 containing sufficient media information to allow it to construct steering files for a content provider's media repertoire. These will be sold to end users using a variety of conventional online or partly online payment techniques.

An example of a suitable steering file format is a SMIL file, commonly used by RealPlayer to organise and synchronise multiple requests for media on remote servers. An example of a SMIL file for this purpose is:

```
<smil><body><par><seq>
<ref src="file://C:\EncryptMedia\MediaKey\clinton.mpeg.rk"/>
<ref src="file://C:\EncryptMedia\Encrypted\clinton.mpeg.em"/>
</seq></par></body></smil>
```

The steering file may alternatively be implemented by a Media Delivery Metafile (MDM) of which the following is an example:

```
<?xml version="1.0" ?>
<MDM Version="1">
<MediaInfo>
```

```
<MEDIAURL>rtsp://localhost/tpkencrypted/ac5e538e.rm</MEDIAURL>
```

<NAME>Greatest Hits - Shining Like A National Guitar/Still crazy after
all these years/Rock</NAME>

<DESCRIPTION>0</DESCRIPTION>

<AUTHOR>Paul Simon</AUTHOR>

<COPYRIGHT></COPYRIGHT>

</MediaInfo>

<KEYSERVER>

<KEYURL>rtsp://localhost/SecureKey/ac5e538e.rk</KEYURL>

<KSPLK>RPK34KHAB22Sz6YOCV4LxM9kLvLNj7HFaCSwO8XBuKq1
YUUm25Vt5w5HNYOfZKqvabQ29

Ei1PuTingVEMEHZEbq-EMImU2_Pk7sNcXTdHh1YQA</KSPLK>

</KEYSERVER>

</MDM>

The SMIL file first causes the user's software (eg RealPlayer) on the client device 10 to send an appropriate request 2 to a key server 3 for the media key corresponding to the media to which the SMIL file relates. The information needed to make this request includes the location of the key server 3 and information that allows the key server to determine which media key is being requested. The process by which this request is made will also include means by which the end user transmits its own public key 4 to the key server 3, and may include transmitting additional identifying or authentication information to the key server. It is preferred that the media key be encrypted using a public key algorithm and it is to facilitate this that the user's public key 4 is provided to the key server.

If the key server 3 verifies, by means external to the present system, that the end user is entitled to receive the requested media key, then the key server 3 encrypts the media key under the end user's public key and sends it 5 to the end user. The end user's software (eg a decrypting "plugin" for RealPlayer) will store the encrypted media key, preferably in volatile memory 6, or alternatively may immediately decrypt

the media key with the end user's private key 15 and store the clear media key in volatile memory. The media key is intended to reside in volatile memory (eg RAM) to make it more secure than if it was stored on a hard drive and to prevent unauthorised repeat use if a pay per view business model is being applied.

5 Upon receipt of the encrypted media key, the steering file 1 then causes the user's software to request 7 a media server 8 to deliver the encrypted media. The media is downloaded 9 and when it arrives (the first encrypted packet in the case of streaming delivery, or the entire encrypted file in the case of download delivery), the media key is retrieved from volatile memory 6, asymmetrically decrypted as already
10 described if it has been stored in encrypted form, and then used to decrypt the media so that it can be viewed or played or otherwise used.

15 In the embodiment just described the retail store 11 constructs, in response to user requests, steering files containing steering information, which may include entitlement information (eg unique electronic "tickets"), obtained in advance from the key server manager. However in another embodiment the retail store may not maintain a stock of such steering information and may instead obtain the information directly from the key server 3 each time it receives a request 2 from a user. The key server 3 could deliver the steering information to the retail store 11 for download to the user or alternatively download the steering information directly to the user client device 10.
20 Verification procedures would still be carried out by the retail store 11 and the key server 3 to verify payment and entitlement respectively.

25 In a third embodiment efficiency gains could be achieved by modifying the second embodiment so that the user would receive a file containing steering information for the media server 8 but instead of steering information for the key server 3, would actually receive in this file an encrypted key. This could be downloaded direct by the key server 3 or via the retail store 11 for forwarding to the user. In such a scenario the steering file information would simply contain the location of the media server and an identifier for the encrypted media selected by the user. As in the first

embodiment the user's software cannot play the encrypted media unless it also is in possession of the key associated with that media to allow it to be decrypted.

The advantages of the system described are:

- (a) only authorised recipients have access to media keys;
- 5 (b) the business and functional responsibilities of managing keys are separated from the responsibilities for managing encrypted media;
- (c) the media keys are delivered to end users "just in time" for them to be used to decrypt the media;
- 10 (d) media keys are not transmitted or stored anywhere other than at a trusted key server unless they have been encrypted under an authorised user's public key;
- (e) the steps required for use of the system by an end user is very simple so that no special knowledge or skill regarding security or encryption techniques is required for end users to use the system.

FOUO 2000-01-01